REMARKS

Claims 28-46 are pending in the application. Claims 1-27 are withdrawn. Of the claims, Claims 28 and 36 are independent claims. Claims 28-46 are rejected under 35 U.S.C. § 102(e) as being deemed anticipated by Ellis (U.S. Patent No. 6,484,257). Claim 44 has been amended to correct a typographical error. The application as argued herein, is believed to overcome the rejection.

The proposed corrected drawings filed on January 26, 2002 have been approved. As requested in the Office Action, corrected drawings are being filed concurrently with this amendment.

The applicants disclose a data encryption system for processing a received data packet. A control process modifies the received packet to include control data that identifies processes to be performed on the packet by a plurality of processors in the system. An interconnection responds to control data in the packet to forward the packet with control data from processor to processor. After processing is complete, the processed packet is forwarded without the control data from an output.

Fig. 8 of the applicant's specification illustrates an embodiment of the applicants' disclosed system for Internet Protocol Security (IPSEC) processing. Referring to Fig. 8, a received packet is modified to include control data which identifies processes (functions, operations) to be performed on the packet. As shown in Fig. 6, the control data is an ordered list of operations to be performed on the received data packet and includes a list of control entries, each of which identifies a process to be performed by a processor on the data packet. Figs. 9A-9D illustrate modification of the control data. Referring to Fig. 9A, at (1), data element 81 adds control data (control 1 and uCode1) identifying that the data packet is to be sent to the IPSEC processor for processing. At (2), the data packet is sent to the IPSEC processor based on the control data added by data element 81. The IPSEC processor adds further control data to the packet indicating further processes to be performed on the data packet by other processors. As shown in Figs. 9C-9D, the packet is forwarded to the other processors 86, 85, 84, 83 in the order specified by the control data added by the IPSEC processor. At (7), after the processed packet 98 including standard protocol headers (IP and ESP) is forwarded without the control data. At

(8), the control data removed from the packet may be provided to the IPSEC processor for monitoring performance. (*See* Page 13, lines 9-17.)

The cited prior art Ellis is related to secure communication sessions in a distributed computing environment. Bandwidth for a secure communication session is increased by assigning a plurality of agents to a client and distributing packets for an application among the agents for processing. As shown in Figs. 5A and 5B, the packet includes standard network protocol headers (IP, TCP, ESP and AH.) (*See* Col. 3, lines 15-24.) The standard IP protocol headers are modified to route encrypted packets between a client and a server through different agents. In order to distribute the data packets, each agent is assigned an IP address and IP headers in the packet are modified by the client 5A10 and the gateway 5A40 to route data packets through different agents to the final destination. The agent performs authentication and encryption/decryption and adds/removes the ESP and AH protocol headers. Referring to Fig. 5A, packet #1 is routed to one agent and packet #2 is routed to another agent 5A70 based on the IP address included in the Agent ID IP header 5A60. As shown in Fig. 5B, if the agent is not the final destination, the agent performs the decryption, removes the ESP and AH headers and forwards the packet which includes IP and TCP protocol headers to the final destination.

In contrast to the applicants' disclosed invention, Ellis merely identifies an agent which will process the packet. Ellis does not suggest a sequence of processes to be applied to a received packet or suggest transferring the received packet from processor to processor in accordance with control data.

Ellis's discussion of standard network protocol headers does not teach or suggest at least the applicants' disclosed "control process which modifies a received packet to include control data which identifies processes to be performed on the packet". Ellis does teach or suggest responding to control data to forward the received packet from "processor to processor" (*see* claim 28) or to perform the processes "in successive processors" (*see* claim 37). Ellis merely discusses modification of standard IP network protocol headers to route packets between a client and a server through a plurality of agents.

Claims 29-36 are dependent on Claim 28 and thus include this limitation over the prior art. Independent Claim 37 and claims dependent on claim 37, include like limitations distinguishing the cited art.

Accordingly, the present invention as now claimed is not believed to be anticipated by or made obvious from the cited art or any of the prior art. Removal of the rejections of claims 28-46 under 35 U.S.C. 102(e) and acceptance of Claims 28-46 is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By Caroline M Fleming

Caroline M. Fleming
Registration No. 45,566
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 1/21/04